

UNITED STATES DISTRICT COURT

for the
Eastern District of Virginia

JAN 19

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Case No. 1:17SW11

INFORMATION ASSOCIATED WITH
UBUYSELLTRADE@AOL.COM THAT IS STORED AT
PREMISES CONTROLLED BY AOL, INC.

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):
See Attachment A (Property to be Searched).

located in the Eastern District of Virginia, there is now concealed (identify the person or describe the property to be seized):
See Attachment B (Particular Things to be Seized).

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
18 U.S.C. §641Offense Description
Violations of Public Money, Property, or Records.

The application is based on these facts:
See attached affidavit.

☐ Continued on the attached sheet.

☒ Delayed notice of 30 days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Reviewed by AUSA/AUSA:

Mike Rich/Andres Vasquez

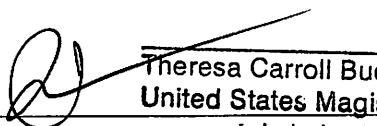


Applicant's signature

Jeffrey Young, Special Agent, NCIS

Printed name and title

Sworn to before me and signed in my presence.

Date: January 19, 2017


Judge's signature

Hon. Theresa Carroll Buchanan, U.S. Magistrate Judge

Printed name and title

City and state: Alexandria, Virginia

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

JAN 19

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
UBUYSELLTRADE@AOL.COM THAT IS
STORED AT PREMISES CONTROLLED
BY AOL, INC.

Case No. 1:17SW11

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Jeffrey Young, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at premises controlled by AOL, Inc, an email provider headquartered at 22000 AOL Way Dulles, VA 20166. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require AOL, Inc to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the Naval Criminal Investigative Service (NCIS) and have been since April 2014. I am a Federal Law Enforcement Officer with the authority to seek search warrants. I am currently assigned to NCISRA Quantico, VA. I am a graduate of both the Criminal Investigator Training Program and Special Agent Basic Training Program at the Federal Law Enforcement Training Center in Glynco, Georgia. Prior to joining NCIS, I was a Police Officer, Investigator, and Sergeant with the Norfolk Police Department in Norfolk,

Virginia for approximately 11 years. I have a bachelor's degree in Business Administration from Saint Leo University.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18 United States Code Section 641-Public Money, Property or Records have been committed by Branden BAKER. There is also probable cause to search the information described in Attachment A for evidence and/or instrumentalities of these crimes further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is a district court of the United States that has jurisdiction over the offense being investigated. 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

6. On June 10, 2016, NCIS was notified of the larceny of several night vision image intensifiers tubes, an item regulated by the International Traffic in Arms Regulations (ITAR), from a supply warehouse onboard Marine Corps Base Quantico. The estimated value of the missing items is approximately \$26,000. An internal audit conducted in May 2016 showed the warehouse was missing three (3) image intensifier tubes with National Stock Number 5855015034799, at a cost of \$5529 each and six (6) image intensifier tubes with National Stock Number 5855015044590, at a cost of \$1650 each.

7. Christopher LIMOX, an active duty Marine, assigned to the supply warehouse, was interviewed as part of this investigation and ultimately admitted to stealing approximately eight image intensifier tubes and claimed it was at the request of Branden Roy BAKER, a former Marine, previously assigned to the same command. LIMOX stated he traded the image intensifier tubes to BAKER for money, equipment and a discount on a firearm. Affiant searched LIMOX's personal email account with his consent and discovered two emails documenting payment from BAKER (associated email: beanmarine83@yahoo.com) to LIMOX via PayPal which corroborated the information provided by LIMOX.

8. A search of ebay.com listings for image intensifier tubes revealed a closed advertisement which listed a New ITT MX-11769 Image Intensifier Autogated for sale. The advertisement was posted by seller known as stsolutionssales, aka Superior Tactical, and listed the location of the seller as Joshua, Texas. The advertisement displayed a photograph of three image intensifier tubes in the original, silver packaging. Affiant sent a copy of the photograph to the manufacturer, Harris Communications. Harris Communications was able to scan the bar codes in the photograph and confirmed that all three of the image intensifier tubes in the photograph were sold to the United States Government and provided the USG Contract Number W9124Q-05-D-0821.

9. On September 1, 2016 and September 9, 2016, BAKER was interviewed by your Affiant. BAKER admitted to stealing image intensifier tubes and other night vision parts from the U. S. Government from approximately 2010 to 2015. BAKER estimated he stole around seventy (70) image intensifier tubes during that time. BAKER reportedly sold, traded and gave away the image intensifier tubes, sometimes as part of a piece of night vision gear and other times just the tube itself. BAKER stated he almost exclusively negotiated the sales via email

after identifying potential buyers on ebay.com (branden00x). BAKER received payment for the stolen government property via his PayPal account (beanmarine83@yahoo.com).

10. BAKER provided his email address beanmarine83@yahoo.com and gave your Affiant consent to assume said email account. BAKER named the following subjects as people to whom he had sold image intensifier tubes and/or night vision parts: Superior Tactical (sales@superiortac.com), Dave JENKINS (davejenkins70@yahoo.com), Kamil JANTON (kamiljanton@gmail.com), Mark KRUGER (119kruger@gmail.com), and James ELSKOE (Ubuyselltrade@aol.com). Your affiant viewed emails exchanged between each of the above listed email address and BAKER which discussed the sale of night vision parts and/or image intensifier tubes. In addition, BAKER gave your Affiant consent to assume his ebay.com account. BAKER's ebay.com account contained a message from KRUGER in which KRUGER stated he had previously bought night vision parts from BAKER via email address vivi519@foxmail.com. Ebay.com records show BAKER received at least two payments in excess of \$1000 from a user with email address vivi519@foxmail.com. Ebay.com also displays the name of the person paying from vivi519@foxmail.com in Chinese letters and a search of ebay.com for user vivi519 shows the user is based in Taiwan. Information provided by BAKER and viewed by your Affiant in the emails from each of the above listed subjects indicate each of them likely purchased the image intensifier tubes and/or night vision parts with the intention of reselling them or transferring them to another individual.

11. Additionally, BAKER's email correspondence shows that he provided the U.S. Government contract number associated with the stolen image intensifier tubes to JANTON, JENKINS and KRUGER, a clear indication that the items they were purchasing belonged to the U.S. Government.

12. Based on the number of image intensifier tubes BAKER admitted to stealing, the period of time over which the thefts occurred, and the volume of emails exchanged pertaining to the transactions in BAKER's own email account, your Affiant believes there to be information related to the thefts in each of the above referenced email accounts along with BAKER's ebay.com account and his PayPal account.

13. In general, an email that is sent to a AOL, Inc subscriber is stored in the subscriber's "mail box" on AOL, Inc servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on AOL, Inc servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on AOL, Inc servers for a certain period of time. Additionally, BAKER suggested he maintained email correspondence as a form of business record and although BAKER has granted access to his email account some deleted content may only be retrievable from AOL, Inc servers.

BACKGROUND CONCERNING EMAIL

14. In my training and experience, I have learned that AOL, Inc provides a variety of on-line services, including electronic mail ("email") access, to the public. AOL, Inc allows subscribers to obtain email accounts at the domain name aol.com, like the email account listed in Attachment A. Subscribers obtain an account by registering with AOL, Inc. During the registration process, AOL, Inc asks subscribers to provide basic personal information. Therefore, the computers of AOL, Inc are likely to contain stored electronic communications (including retrieved and unretrieved email for AOL, Inc subscribers) and information concerning subscribers and their use of AOL, Inc services, such as account access information, email transaction information, and account application information. In my training and experience,

such information may constitute evidence of the crimes under investigation since the information can be used to identify the account's user or users.

15. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

16. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

17. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

18. This application seeks a warrant to search all responsive records and information under the control of AOL, Inc, a provider subject to the jurisdiction of this court, regardless of where AOL, Inc has chosen to store such information. The government intends to require the disclosure pursuant to the requested warrant of the contents of wire or electronic communications and any records or other information pertaining to the customers or subscribers if such communication, record, or other information is within AOL, Inc's possession, custody, or control, regardless of whether such communication, record, or other information is stored, held, or maintained outside the United States.¹

¹ It is possible that AOL, Inc stores some portion of the information sought outside of the United States. In Microsoft Corp. v. United States, 2016 WL 3770056 (2nd Cir. 2016), the Second Circuit held that the government cannot enforce a warrant under the Stored Communications Act to require a provider to disclose records in its custody and control that are stored outside the United States. As the Second Circuit decision is not binding on this court, I respectfully request that this warrant apply to all responsive information—including data stored outside the United States—pertaining to the identified account that is in the possession, custody, or control of AOL, Inc. The government also seeks the disclosure of the physical location or locations where the information is stored.

19. As explained herein, information stored in connection with an email account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user’s account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Additionally, stored electronic data may provide relevant insight into the email account owner’s state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner’s motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

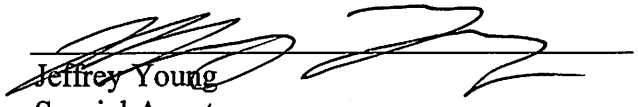
CONCLUSION

20. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on AOL, Inc, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

REQUEST FOR SEALING

21. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

Respectfully submitted,


Jeffrey Young
Special Agent
NCIS

Subscribed and sworn to before me on 1/19/17, 2017


Sa Carroll Buchanan
United States Magistrate Judge
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with an email address (ubuyselltrade@aol.com) that is stored at premises owned, maintained, controlled, or operated by AOL, Inc, a company headquartered at 22000 AOL Way Dulles, VA 20166.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by AOL, Inc (the “Provider”)

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held or maintained inside or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. The types of service utilized;
- d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken; and

f. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

The Provider is hereby ordered to disclose the above information to the government within **14 days** of the issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence and/or instrumentalities of violations of Title 18 United States Code Section 641-Public Money, Property, or Records those violations involving Branden BAKER and occurring after **01Jan2010**, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- (a) The sale or purchase of image intensifier tubes or night vision parts, payments and/or trades made in exchange for image intensifier tubes or night vision parts, use for or disposition of image intensifier tubes or night vision parts, communications regarding the source or origin of the image intensifier tubes or night vision parts
- (b) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;
- (c) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;
- (d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).
- (e) The identity of the person(s) who communicated with the user ID about matters relating to theft and sale of government property, namely image intensifier tubes and night vision parts, including records that help reveal their whereabouts.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
BUSINESS RECORDS PURSUANT TO FEDERAL RULE
OF EVIDENCE 902(11)**

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by AOL, Inc, and my official title is _____. I am a custodian of records for AOL, Inc. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of AOL, Inc, and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

- a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;
- b. such records were kept in the ordinary course of a regularly conducted business activity of AOL, Inc; and
- c. such records were made by AOL, Inc as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

Date

Signature